Lobachevskii Journal of Mathematics 2016 vol.37 N3, pages 234-239

Towards an operad-based cryptography: Applications of commutative operads

Gaynullina A., Tronin S.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© 2016, Pleiades Publishing, Ltd.In this paper we show the use of commutative operads in public-key cryptography. Commutative operads were introduced by S.N. Tronin in 2006. They are a special case of algebraic operads and a natural generalization of commutative algebraic theories. We consider some cryptographic protocols based on commutative operads. For the protocol of the creation a common secret key, we describe and investigate its implementation and cryptographic security in particular cases.

http://dx.doi.org/10.1134/S1995080216030100

Keywords

algebra over an operad, algebraic cryptography, authentication, cipher, commutative operad, cryptographic protocol, digital signature, Operad, secret key, security, tropical semiring